المدرسة المغربية لعلوم الهندسة في اعلاميات التسيير والاعلاميات الصناعية



Ecole Marocaine
des Sciences de l'Ingénieur

EMSI

**Mini Projet**

# Virtual Private Network
## Etude comparative et réalisation d´un VPN MPLS


**Réalisé par :**
**NOUCHTI Ouafa**
**El QASMI Med Zakaria**
**HILALI Tarik**

**Encadré par :**
**Mr : ISMAILI Rachid**





***Promotion : IRT5*** ***Année universitaire 2009/2010***

بسم الله الرحمن الرحيم

"وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ"

*التوبة آية 105*

"صدق الله العظيم"

# Dédicaces

*Nous dédions ce travail :*

*A nos chers parents pour leur amour, sacrifice et soutiens.*

*A nos collègues pour leur compréhension et fidélité.*

*A nos enseignants pour leurs efforts remarquables.*

*A ceux à qui nous devons reconnaissance.*

*A ceux qui nous font partager joies et souffrances.*

*Qu'ils trouvent tous ici nos sincères gratitudes et reconnaissances.*

...

# Remerciements

*Avant d'entamer le vif de notre travail, il nous est tellement agréable de présenter nos sincères remerciements au personnel de l'EMSI.*

*Nous tenons également à exprimer notre reconnaissance à notre professeur encadrant Mr. Rachid ISMAILI qui nous a beaucoup encouragés, pour son aide et orientation durant la période du projet, il a engagé son temps et ses conseils pour nous venir en aide. Nos vifs remerciements sont également adressés à tous les professeurs de l'EMSI.*

*Enfin, notre profonde gratitude et notre respect a toute personne qui a contribué de prés ou de loin à l'élaboration de ce travail.*

# Abstract


Published by the IETF in 1997, MPLS technology first emerged within the networking industry for IP core networks primarily as a mechanism to provide VPN services and traffic engineering capabilities.

MPLS is now being extended toward the Ethernet/optical and access-network segments to extend the benefits realized in the core and provide a true end-to-end architecture for the delivery of packet data services.

This article will present an overview of the operation of MPLS, then an example of configuration the Cisco router.

# Sommaire

**Introduction générale.** 1

**Chapitre 1 : Généralités sur les VPNs.** 2

1.1 Mode de fonctionnement des VPNs 2

1.1.1 Généralités. 2

1.2 Les types d'utilisation de VPNs. 3

1.2.1 Le VPN d'accès. 3

1.2.2 L'intranet VPN. 4

1.2.3 L'extranet VPN. 4

1.3 Les Protocoles utilisés. 5

1.3.1 PPTP (Point to Point Tunneling Protocol). 5

1.3.2 P2TP (Layer 2 Tunneling Protocol). 6

1.3.3 IPSec (IP Security). 7

1.3.4 Comparaison entre le PPTP et le T2LP / IPSec. 8

1.3.5 MPLS/VPN. 9

1.3.5.1 Introduction. 9

1.3.5.2 Principe de Fonctionnement. 12

1.3.6 Comparaison entre MPLS et IPSec. 17

**Chapitre 2 : Réalisation.** 19

2.1 Présentation du logiciel GNS3. 19

2.2 Description de la maquette. 20

2.2.1 L'activation du routage. 21

2.2.2 L'activation du MPLS. 21

2.2.3 L'activation du MPLS VPN. 22

2.3 Configuration d'un VPN MPLS. 22

**Conclusion Générale** 30

**Bibliographie.** 31

**Annexes.** 32

# Glossaire

**A**

**ASIC** Application Specific Interface Circuits
**ATM** Asynchronous transfer mode

**B**

**BGP** Border Gateway Protocol

**C**

**CEF** Cisco Express Forwarding

**D**

**Diffserv** Differentiated Services
**DSCP** Differentiated Services Code Point

**E**

**EGP** Exterior Gateway Protocol
**EIGRP** Enhanced Interior Gateway Routing Protocol

**F**

**FR** Frame Relay
**FEC** Forwarding Equivalency Class

**G**

**GRE** Generic Routing Encapsulation

**I**

**Intserv** Integrated Services
**IGP** Interior Gateway Protocol
**IGRP** Interior Gateway Routing Protocol
**ISIS** Intermediate System-to-Intermediate System
**ISP** Internet Service Provider

**L**

**LDP** Label Distribution Protocol
**LSP** Label Switching Path
**LSR** Label Switching Router

**M**

**MPLS** **Multi Protocol Label Switching**
**MP-BGP** MultiProtocol-Exterior Gateway Protocol
**MTU** Maximum Transmission Unit

**O**

**OSPF** Open Shortest Path First

**P**

**PPP** Point to Point Protocol
**POP** Point of Presence
**PHP** Penultimate Hop Popping

**Q**

**QoS** Quality of Service

**R**

**RD** Route distinguishers
**RIP** Routing Information Protocol
**RSVP** Ressource Reservation Protocol
**RT** Route Targets

**S**

**SDH** Synchronous Digital Hierarchy

**T**

**TDP** Tag Distribution Protocol
**TE** Traffic Engineering
**TTL** Time to Live

**V**

**VPN** Virtual private Network
**VRF** VPN Routing and Forwarding

**W**

**WDM** Wavelength Division Multiplexing

# Liste des figures

**Figure 1.1:** Schéma générique de Tunnelisation. 3

**Figure 1.2:** VPN d'accès. 4

**Figure 1.3:** L'intranet VPN. 4

**Figure 1.4:** L'extranet VPN. 4

**Figure 1.5:** Principe d'encapsulation PPTP. 6

**Figure 1.6:** Principe d’encapsulation L2TP. 7

**Figure 1.7:** VPN/MPLS. 9

**Figure 1.8:** Overlay model. 10

**Figure 1.9:** Peer to peer model. 11

**Figure 1.10:** Principe de fonctionnement(1). 13

**Figure 1.11:** Principe de fonctionnement(2). 14

**Figure 1.12:** récapitulatif VPN/MPLS. 16

**Figure 2.20:** Maquette réalisée. 20

**Figure 2.21:** Commande « traceroute » exécutée au niveau du routeur CEB avec l’adresse 10.0.0.1 26

**Figure 2.22:** Commande « traceroute » exécutée au niveau du routeur CEA avec l’adresse 10.0.6.2 27

**Figure 2.23:** Commande « Show ip vrf » exécutée au niveau du routeur PEB. 27

**Figure 2.24**: Commande « Show ip vrf interfaces » exécutée au niveau du routeur PEA. 27

**Figure 2.25:** Commande « Show mpls forwarding-table » exécutée au niveau du routeur PEB. 28

**Figure 2.26:** Commande « Show ip cef vrf emsi 10.0.6.2 detail » exécutée au niveau du routeur PEA. 28

# Liste des tableaux

**Tableau 1.1 :** Comparaison entre MPLS et IPSec 17

**Tableau 2.2 :** Configuration du routeur CEA 22

**Tableau 2.3 :** Configuration du routeur PEA 23

**Tableau 2.4 :** Configuration du routeur PEB 24

**Tableau 2.5 :** Configuration du routeur CEB 25

**Tableau 2.6 :** Configuration du routeur P 25

# Introduction générale

Au début de l'Internet, la préoccupation majeure était de transmettre les paquets à leur destination. Ensuite, des mécanismes inhérents à TCP ont été développés pour faire face aux conséquences induites par les pertes de paquets ou la congestion du réseau. Mais depuis le début des années 1990, la communauté des fournisseurs de service (ISP : Internet service Provider) qui administrent l'Internet est confrontée non seulement au problème de croissance explosive mais aussi à des aspects de politique, globalisation et stabilité du réseau.
Par ailleurs, outre ces différents aspects, apparaît une très forte diversification des services offerts. Ainsi de nouvelles applications se développent sur le réseau : téléphonie, vidéoconférence, diffusion audio et vidéo, jeux en réseau, radio et télévision en direct…
L'émergence des réseaux privés virtuels (VPN), nécessite également une différentiation de services. La qualité de service de bout en bout apparaît, dans ce contexte, essentielle au succès de ces applications.

Avec l'arrivée de la technologie MPLS et les modèles de gestion de la qualité de service (Diffserv et Intserv) une nouvelle approche est considérée (MPLS pour l'augmentation des performances des équipements réseaux, les notions de trafic engineering et les VPN et la gestion de qualité de service pour le traitement de la congestion, la classification des trafics et la garantie de service).
Du point de vue ISP, considéré comme le client principal du backbone IP et la passerelle des utilisateurs Internet et réseaux, un défit est à surmonter c'est d'assurer une liaison parfaite entre ses sites à travers le backbone. Plusieurs solutions existent dont la plus innovante est MPLS VPN.

Cette étude est composée de 2 chapitres. Le premier chapitre présente les VPN son principe de fonctionnement, ses nouveaux concepts et ses atouts.
Le deuxième chapitre contient la réalisation de la maquette de simulation VPN/MPLS.





Chapitre 1 :

# Généralités sur les VPNs

- **Mode du Fonctionnement des VPNs**
- **Les types d'utilisation de VPN**
- **Protocoles utilisés**

# Chapitre 1 : Généralités sur les VPNs

## Introduction

Les entreprises ont des réseaux locaux de plus en plus importants qui comportent des applications et des données essentielles à l'entreprise. Le problème qui se pose est le suivant : comment des succursales d'une entreprise peuvent-elles accéder à ces données alors qu'elles sont réparties sur de grandes distances géographiques. Pour pallier à ce problème, ces entreprises mettent en place un réseau VPN.

Nous verrons dans cet article le principe de fonctionnement du VPN. Nous nous intéresserons aussi aux différents types d'utilisation du VPN et aux protocoles permettant sa mise en place.

## 1.1 Mode de fonctionnement des VPNs

### 1.1.1 Généralité

Les réseaux privés virtuels reposent sur des protocoles nommés « protocoles de tunneling », (ou encore protocoles de tunnelisation). Ils ont pour but de sécuriser le réseau en cryptant les données partant des extrémités du VPN à l'aide d'algorithmes de cryptographie.

On utilise le terme « Tunnel » pour représenter le passage sécurisé dans lequel circulent les données cryptées. Ainsi, toute personne n'étant pas connectée au VPN ne peut pas décrypter ces données.

Lorsqu'un utilisateur veut accéder aux données sur le VPN, on appelle client VPN (Client d'Accès Distant) l'élément qui chiffre et déchiffre les données du côté client et serveur VPN (Serveur d'Accès Distant) l'élément qui chiffre et déchiffre les données du côté du serveur (dans notre cas, c'est l'entreprise).

Une fois le serveur et le client identifiés, le serveur crypte les données et les achemine en empruntant le passage sécurisé (le tunnel), les données sont ensuite décryptées par le client et l'utilisateur a accès aux données souhaitées.





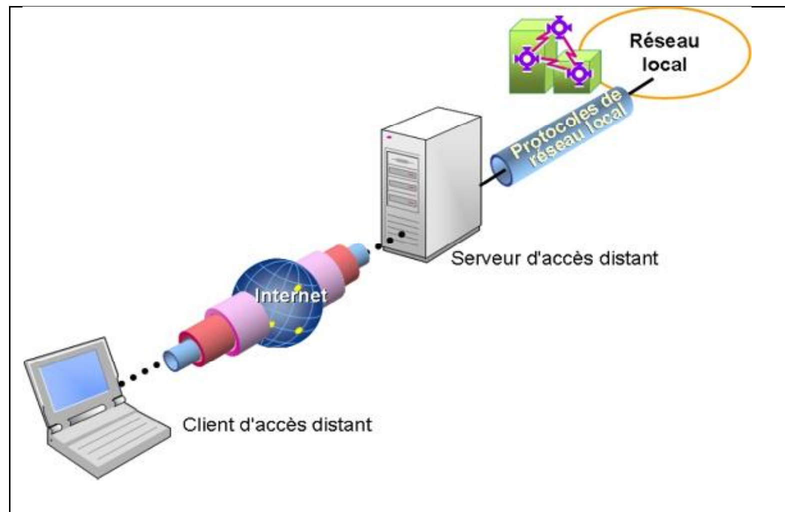



**Figure 1.1 :** Schéma générique de Tunnelisation

## 1.2 Les types d'utilisation de VPN

Dans cette partie, nous étudierons les 3 types d'utilisation du VPN qui sont :

- Le VPN d'accès
- L'intranet VPN
- L'extranet VPN

### 1.2.1 Le VPN d'accès

Le VPN d'accès est utilisé pour permettre à des utilisateurs d'accéder au réseau privé de leur entreprise. L'utilisateur se sert de sa connexion Internet pour établir la connexion VPN

On a deux cas :

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.

- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

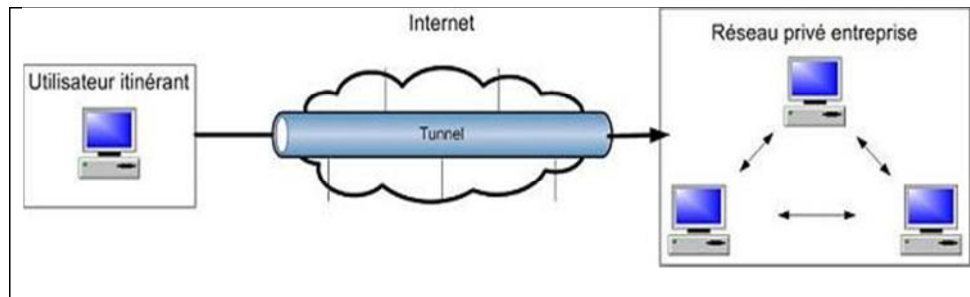



**Figure 1.2 :** VPN d'accès

### 1.2.2 L'intranet VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

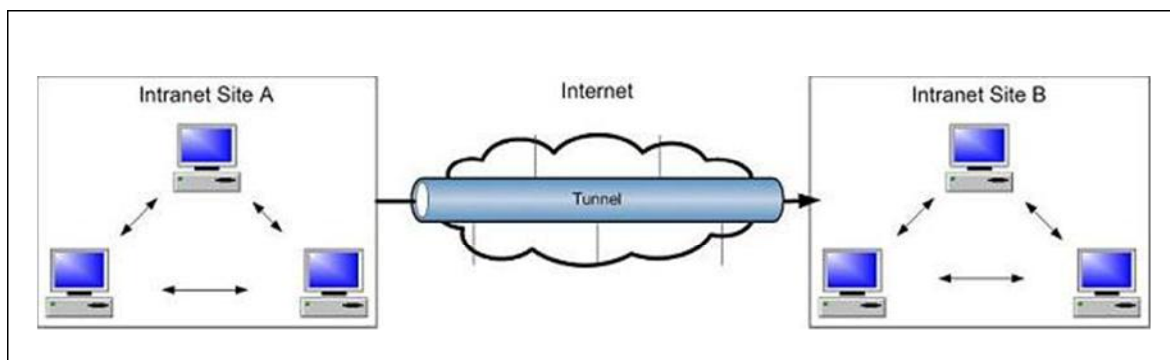



**Figure 1.3 :** L'intranet VPN

### 1.2.3 L'extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

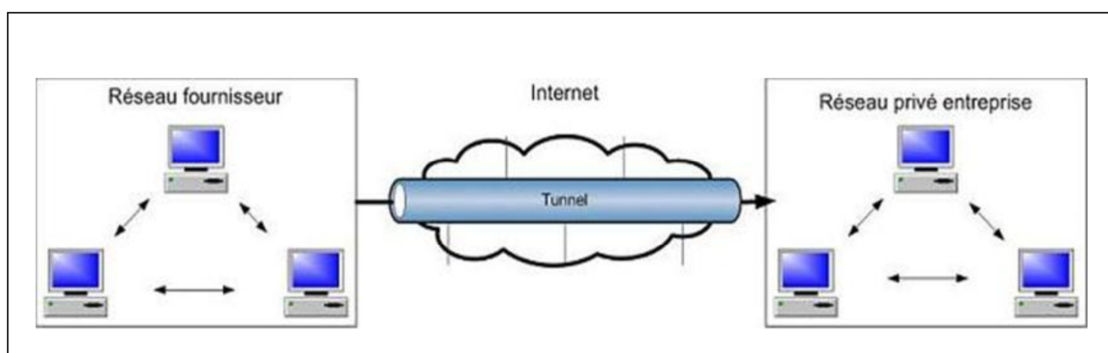



**Figure 1.4 :** L'extranet VPN

## 1.3 Protocoles utilisés

Il existe deux catégories de protocoles, les protocoles de niveau 2 et 3.

Nous avons 3 protocoles de niveau 2 pour réaliser des VPN : le PPTP (de Microsoft), le L2F (développé par CISCO) et le L2TP. Nous parlerons ici que du PPTP et du L2TP car le L2F est un protocole quasi obsolète.

Il existe aussi un protocole de niveau 3, le IPSec qui permet de transporter des données chiffrées pour les réseaux IP.

### 1.3.1 PPTP (Point to Point Tunneling Protocol)

Le principe du protocole PPTP est de créer des trames sous le protocole PPP et de les encapsuler dans des datagrammes IP. PPTP crée ainsi un tunnel de niveau 3 défini par le protocole GRE (Generic Routing Encapsulation).

Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur.

L'établissement d'une connexion se déroule en deux étapes :

- Le client effectue d'abord une connexion avec son FAI (Fournisseur d'accès à Internet).
  Cette première connexion établie une connexion de type PPP et permet de faire circuler des données sur Internet.

- Par la suite, une deuxième connexion dial-up est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP.

Ainsi, le trafic conçu pour Internet emprunte la connexion physique normale et le trafic conçu pour le réseau privé distant passe par la connexion virtuelle de PPTP.

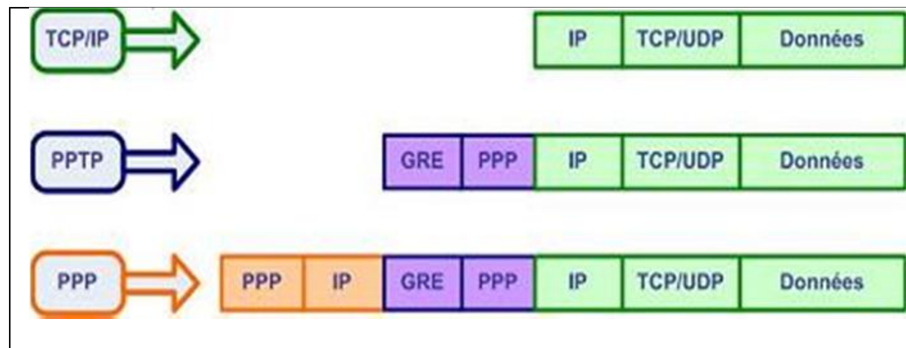



**Figure 1.5:** Principe d'encapsulation PPTP

Il existe ensuite d'autres protocoles qui peuvent être associé à PPTP afin de sécuriser les données ou de les compresser. Mais nous ne nous s'attarderons pas sur ces différents protocoles.

## 1.3.2 P2TP (Layer 2 Tunneling Protocol)

Le protocole L2TP est issu de la convergence des protocoles PPTP et L2F. Ainsi le protocole L2TP encapsule des trames PPP, encapsulant elles-mêmes d'autres protocoles tels que IP mais aussi IPX ou encore NetBIOS.

Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet.

L2TP repose sur deux concepts :

- les concentrateurs d'accès L2TP (LAC) : Ces périphériques LAC fournissent un support physique aux connexions L2TP. Le trafic étant alors transféré sur les serveurs réseau L2TP. Ces serveurs peuvent s'intégrer à la structure d'un réseau commuté RTC ou alors à un système d'extrémité PPP prenant en charge le protocole L2TP. Ils assurent le fractionnement en canaux de tous les protocoles basés sur PPP. Le LAC est l'émetteur des appels entrants et le destinataire des appels sortants.
- les serveurs réseau L2TP (LNS) : Le LNS gère le protocole L2TP côté serveur. Le protocole L2tp n'utilise qu'un seul support, sur lequel arrivent les canaux L2TP. Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface PPP du concentrateur d'accès Lac.

Le LNS est l'émetteur des appels sortants et le destinataire des appels entrants. C'est lui qui sera responsable de l'authentification du tunnel.

L2TP n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi on l'utilise très souvent avec le protocole IPSec.

On distingue principalement 2 composantes dans les paquets L2TP :

- Les paquets d'information, encapsulés dans des paquets PPP pour les sessions utilisateurs qui servent pour le transport de L2TP.
- Le protocole de signalisation, qui utilise le contrôle de l'information L2TP est encapsulé dans des paquets UDP/IP.

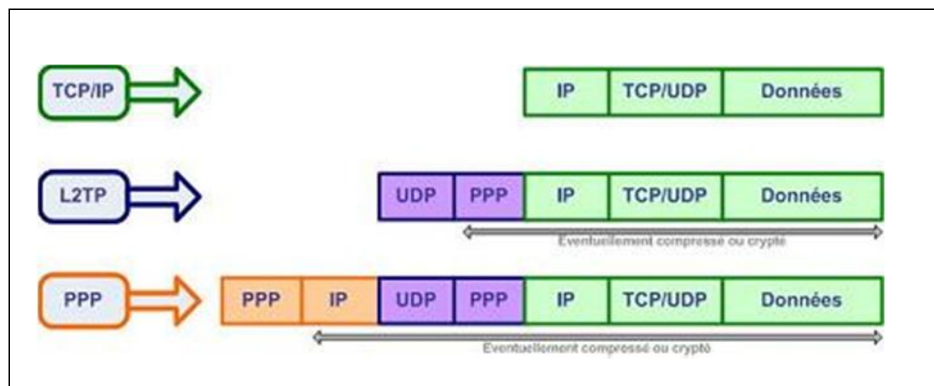



**Figure 1.6:** Principe d'encapsulation L2TP

## 1.3.3 IPSec (IP Security)

IPSec est un protocole qui permet de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.
Le protocole IPSec est basé sur trois modules :

- Le premier, Authentification Header (AH) vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité.
- Le second, Encapsulating Security Payload (ESP) peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des

informations. Ces deux premiers mécanismes sont presque toujours utilisés conjointement.

- Le troisième, Internet Key Exchange (IKE) permet de gérer les échanges ou les associations entre protocoles de sécurité.

Le protocole IPSec est souvent utilisé avec le L2TP.

### 1.3.4 Comparaison entre PPTP, T2LP et IPSec

PPTP présente l'avantage d'être complètement intégré dans les environnements Windows. Cependant comme beaucoup de produit Microsoft la sécurité est le point faible du produit :

- Mauvaise gestion des mots de passe
- Faiblesses dans la génération des clés de session
- Faiblesses cryptographiques
- Identification des paquets non implémentée

L2TP / IPSec sont plus robustes en terme de sécurité que l'utilisation du PPTP.

Les points négatifs de L2TP / IPSec sont les suivants :

- L'ensemble des équipements d'un VPN L2TP doit bien implémenter le protocole IPSec.
- IPSec ne permet d'identifier que des machines et non pas des utilisateurs.
- IPSec à cause de la lourdeur des opérations de cryptage/décryptage réduit les performances globales des réseaux.
- L'achat de périphériques dédiés, coûteux est souvent indispensable.

## 1.3.5 MPLS/VPN

### 1.3.5.1 Introduction

Les VPN/MPLS sont essentiellement implémentés chez les opérateurs afin de fournir des services à leurs clients. Les opérateurs utilisent leur backbone sur MPLS pour créer des VPN, par conséquent le réseau MPLS des opérateurs se trouve partagé ou mutualisé avec d'autre client.

Du point de vue du client, il a l'impression de bénéficier d'un réseau qui lui est entièrement dédié. C'est-à-dire qu'il a l'impression d'être le seul à utiliser les ressources que l'opérateur lui met à disposition. Ceci est dû à l'étanchéité des VPN/MPLS qui distingue bien les VPN de chaque client et tous ces mécanismes demeurent transparents pour les clients.

Finalement, les deux parties sont gagnantes car les clients ont un véritable service IP qui leur offre des VPN fiables à des prix plus intéressants que s'ils devaient créer eux-mêmes leur VPN de couche 2. Les opérateurs eux aussi réduisent leurs coûts du fait de la mutualisation de leurs équipements.

Voici une représentation des VPN/MPLS.

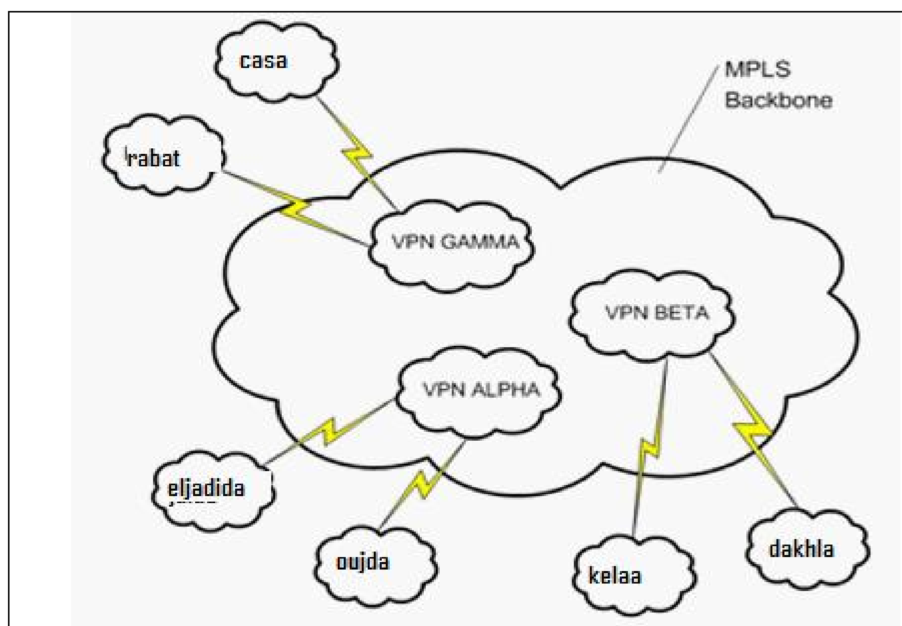



**Figure 1.7 :** Représentation des VPN/MPLS.

Au lancement des VPN/MPLS le modèle Overlay avait été choisi, il consiste à émuler des lignes dédiées entre chaque entité du client sur le réseau MPLS. Il s'agit en fait d'un LSP (Label Switched Path) sur le réseau MPLS qui relie chaque site. La création de ces LSP entre les différents sites de l'entreprise permettra alors de former un VPN IP.

**Overlay model**

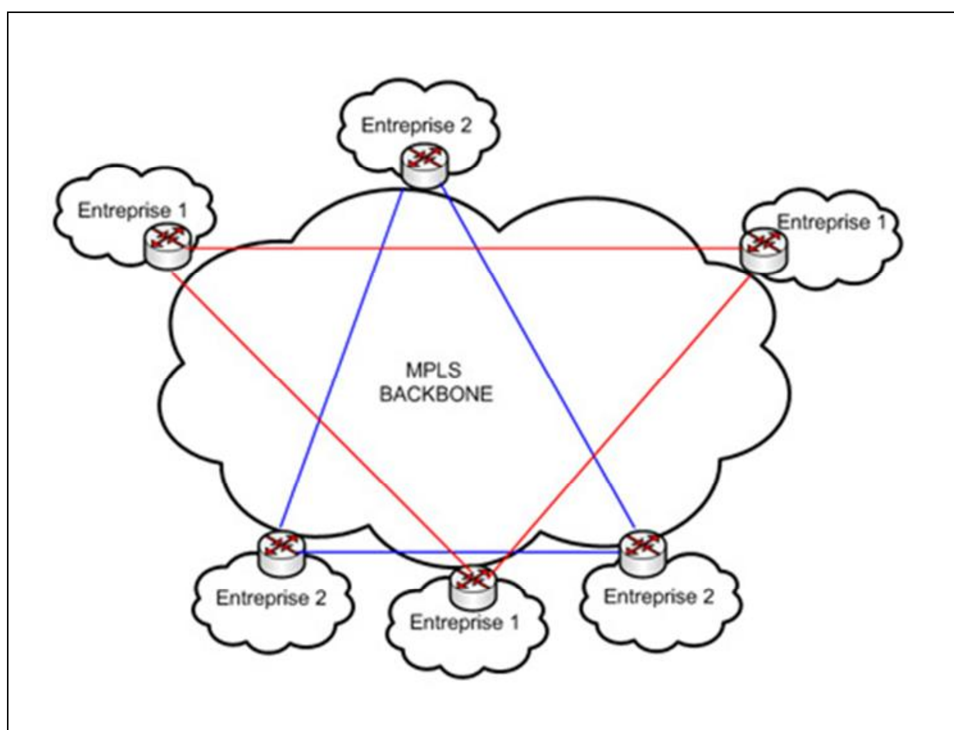



**Figure 1.8:** Overlay model

Ce modèle a cependant un inconvénient car les points d'accès au réseau MPLS se situent dans le réseau du client. En effet, l'ajout de nouveaux sites dans ce VPN nécessite la création de nouveaux LSP. Ce modèle pose ainsi un problème de scalabilité. Si nous avons 5 sites appartenant à un VPN, l'ajout d'un 6ième site requiert la mise en place de 5 nouveaux LSP. Par conséquent, plus le nombre de sites est élevé plus la tache s'avère fastidieuse.

Un autre modèle résout ce problème de scalabilité, il s'agit du modèle « peer to peer ». Ainsi, l'ajout d'un grand nombre de sites ne pose pas de difficulté.

D'autre part, les points d'accès au réseau MPLS, de ce modèle, se trouvent cette fois ci du coté de l'opérateur sur les équipements PE (Provider Edge router). Chaque site échange avec

les équipements PE des informations de routage et l'opérateur achemine par la suite les données vers les sites de destination sur son réseau MPLS.

**Peer to peer model**

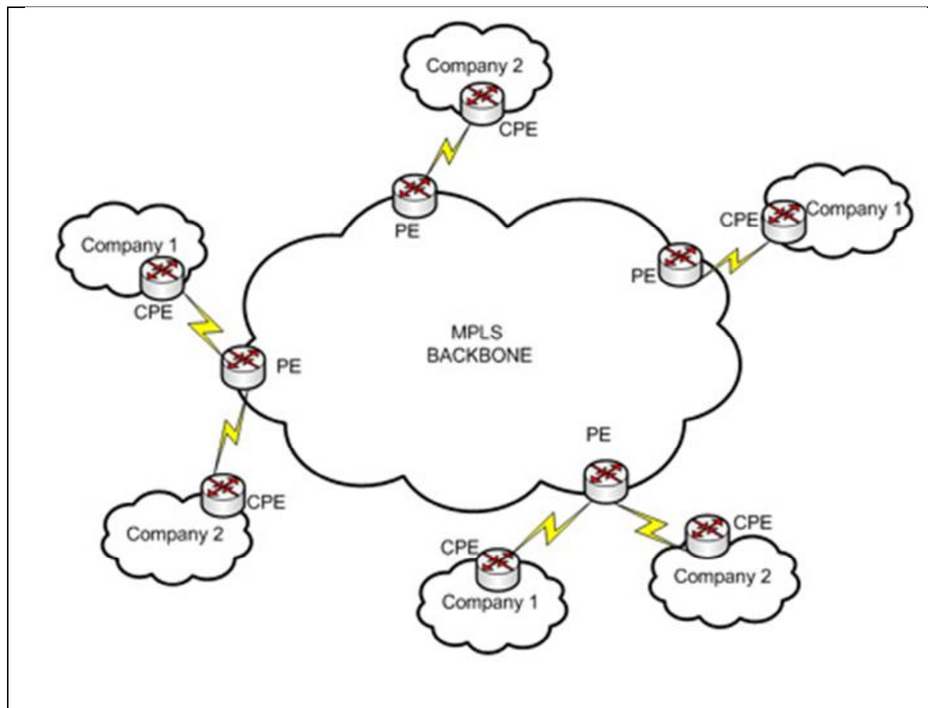



**Figure 1.9:** Peer to peer model

Actuellement ce modèle est largement employé chez les opérateurs car il permet l'ajout de nouveaux sites en changeant la configuration des PE. De plus, du point de vue de l'utilisateur l'interconnexion avec le VPN ne se fait que sur un seul équipement de l'opérateur contrairement au modèle Overlay, il s'agit du PE. Enfin, le routage entres différents sites clients est optimale car le PE connaît sa topologie et peut de ce fait choisir la route adéquate.

De manière générale, la topologie utilisée pour relier les sites dans un VPN avec ce modèle est la topologie entièrement maillée ou « full mesh ». Cela implique que tous les sites peuvent se voir ou bien qu'il existe une liaison point à point entre tous les sites du VPN.

## 1.3.5.2 Principe de fonctionnement

Durant la conception d'un réseau d'entreprise, les ingénieurs choisissent généralement des plages d'adresses IP privées pour leur réseau LAN (10.0.0.0, 172.16.0.0, 192.168.0.0). Or le réseau MPLS permet l'implémentation de plusieurs VPN clients au sein de son réseau. Il faut par conséquent trouver un moyen de différencier les VPN qui peuvent avoir le même adressage IP. La notion de « route distinguisher » ou RD est alors introduite afin de différencier les différentes routes qui circulent sur le réseau MPLS.

Cette route distinguisher d'une taille de 8 octets est ajoutée au préfixe ipv4 (de 4 octets) pour étendre l'adressage IP. La taille de cette adresse fait donc 96 bits en tout.
Le format de cette adresse devient alors : RD : préfixe IPV4

Cette extension de l'adresse IP nous permet de différencier les différentes plages d'adresses, elle nous permet également de différencier les différents VPN.

De plus, pour rendre la communication inter VPN interdite, la technologie MPLS implémente des tables de routages spécifiques à chaque VPN. Ces tables de routage appelées VRF (Virtual Routing and Forwarding table) se réfèrent aux identifiants de chaque VPN, les RD. De cette façon chaque VPN possèdent leur propre table de routage ou VRF dans le réseau MPLS et ne voient pas les autres routes accessibles sur le réseau MPLS.

Néanmoins il existe une certaine flexibilité sur ces VRF, car dans le cas ou l'on souhaite implémenter un extranet par exemple, un site peut alors appartenir à plusieurs VPN. Mais, cela ne change rien au fait que le routage est impossible entre deux VPN différents.

Les CPE (Customer Premises Equipment) des sites utilisateurs sont connectés au PE de l'opérateur pour appartenir au VPN. Ensuite les VRF des VPN en question doivent être configurés sur les interfaces des PE pour que les sites soient bien reliés à cette VRF ou encore à ce VPN.

Suivant leurs configurations les PE peuvent alors avoir plusieurs interfaces configurées pour plusieurs VRF. Il en résulte donc que les PE peuvent avoir plusieurs tables de routage pour chaque VPN. De plus, nous pouvons préciser que ces tables de routage VRF sont mises à jours en parallèle avec la table de routage principale du PE ou nœud Edge-LSR.

Pour rappel, cette table de routage principale sert à atteindre les autres nœuds LSR au sein du réseau MPLS. Elle est remplie par un protocole de routage IGP et sert à mettre à jour la LFIB qui fait la correspondance entre les FEC et les labels.

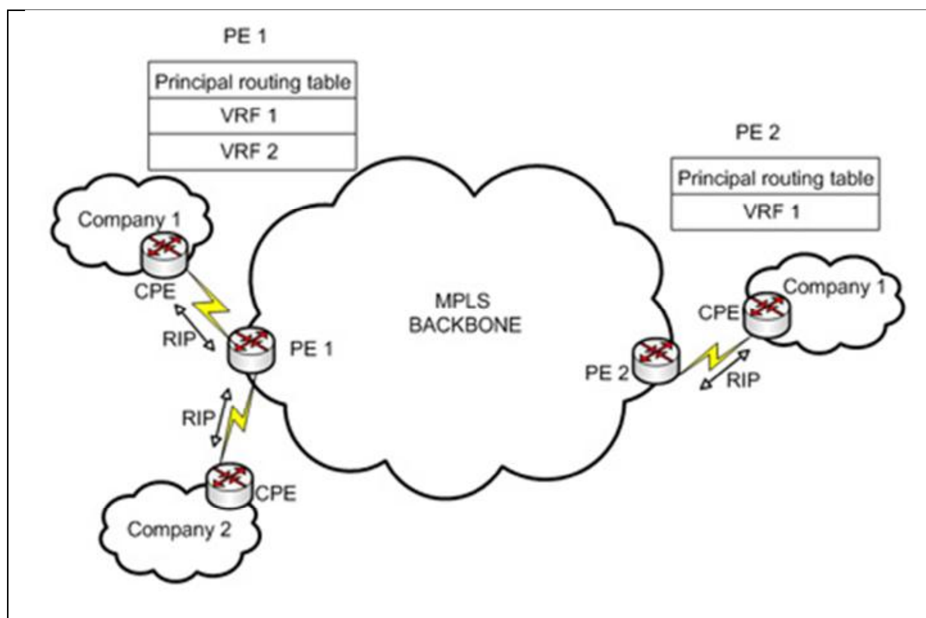



**Figure 1.10 :** Principe de fonctionnement(1)

Sur la figure précédente les sites connectés au VPN matérialisant la connexion CPE - PE peuvent communiquer avec l'intermédiaire d'une route statique ou encore RIP v2, OSPF BGP… pour envoyer leurs informations vers le PE de l'opérateur. Dans notre exemple nous utilisons le protocole RIP v2.

Jusqu'à présent nous avons vu comment les sites clients envoyaient leurs informations vers les PE et comment les PE gérer ces différents VPN. Maintenant nous allons nous intéresser à la communication des sites clients mais du coté backbone MPLS.

Nous avons vu plus haut que les nœuds LSR utilisent un protocole IGP pour connaître leurs voisins dans le réseau MPLS. Cela leur permettait de renseigner leur table LIB faisant l'association des FEC avec les labels.

D'autre part, un protocole de distribution de label est utilisé pour échanger les labels et effectuer des mapping entre les nœuds LSR pour établir un LSP. Mais avec les VPN il y a eu l'introduction du RD (Route Distinguisher) afin de distinguer les différents VPN.

Il a été décidé que pour les VPN implémentés sur les réseaux MPLS, le protocole d'échange de label serait le MP-BGP (MultiProtocol – Border Gateway Protocol). Des sessions BGP sont établies entre deux nœuds Edge-LSR (ou PE) et non entre un PE et un LSR (ou P router). Car en effet, entre le PE et les P router, le mécanisme qui s'applique est le « label swapping ». Les sessions BGP sont donc effectuées entre les différents PE pour échanger les labels faisant l'association entre les labels et les VRF.

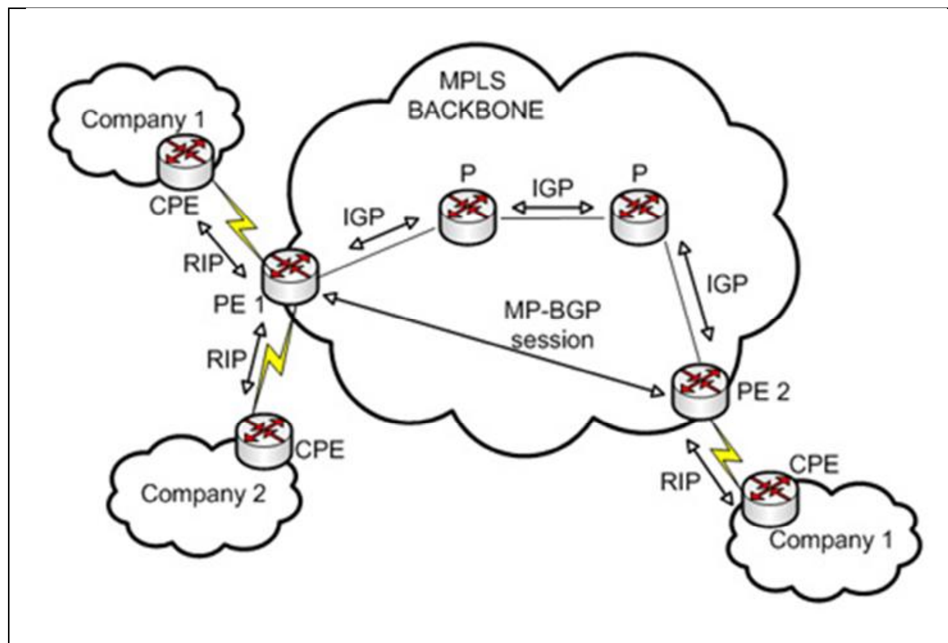



**Figure 1.11 :** Principe de fonctionnement(2)

Lorsqu'un PE apprend une nouvelle route :

- Il insère dans sa VRF et indique qu'il sait la joindre en RIP.
- Ensuite il annonce cette route avec les autres PE en établissant une session BGP en fournissant le label associé pour pouvoir atteindre ce VPN en question.
- Enfin, seul les PE sur lesquels les VRF ont été configurées vont rajouter ces routes dans leur table de routage.

Dès lors qu'il y a un transport de données entre les VPN, les CPE envoient les paquets aux PE avec lesquels ils sont connectés. Les PE identifient à quels VPN ces CPE font parties, ensuite ils consultent leur VRF et insèrent le label qui est associé au préfixe IP de destination et qui fait également partie de ce VPN.

Par la suite, la notion de pile de labels ou « stack label » intervient. Le label dont vous venons de parler juste avant est déjà inséré sur les paquets, il nous sert à identifier vers quel VPN nous devons communiquer. Mais lors de la traversée du cœur de réseau MPLS, nous avons des labels supplémentaires insérés en haut de la pile pour pouvoir acheminer les données d'un noeud LSR à un autre. Ces nouveaux labels nous servent à transférer les données durant le processus de « label swapping ». Ces labels sont donc commutés à chaque saut entre les nœuds LSR et ces nœuds ne s'occupent pas des labels situés en dessous du label en haut de pile.

A l'arrivée sur le nœud Edge-LSR, le nœud LSR qui vient de lui envoyé les données a auparavant retiré le label nécessaire au mécanisme de label swapping. Le nœud Edge-LSR se retrouve ainsi avec des données mais possédant encore le label du VPN. Le nœud Edge-LSR n'a plus qu'à identifier la valeur du VPN de retirer ce dernier label et transferer les données à l'extérieur du réseau MPLS. Ces données sont finalement envoyées vers le CPE relié au VPN identifié juste avant.

Remarque : Il se peut que des PE se situent dans le même LAN et que pour envoyer les données du site 1 vers le site 2 ils n'aient pas besoin de passer par un P router. Le transfert se fait alors de PE à PE directement car il s'agit du chemin optimal. Ce procédé est le « Penultimate Hop Popping » qui consiste à retirer des labels avant l'envoi des données vers le nœud egress. Cela évite ainsi que le nœud egress ait 2 fois à consulter les labels et l'entête IP de destination pour forwarder les données utilisateurs.

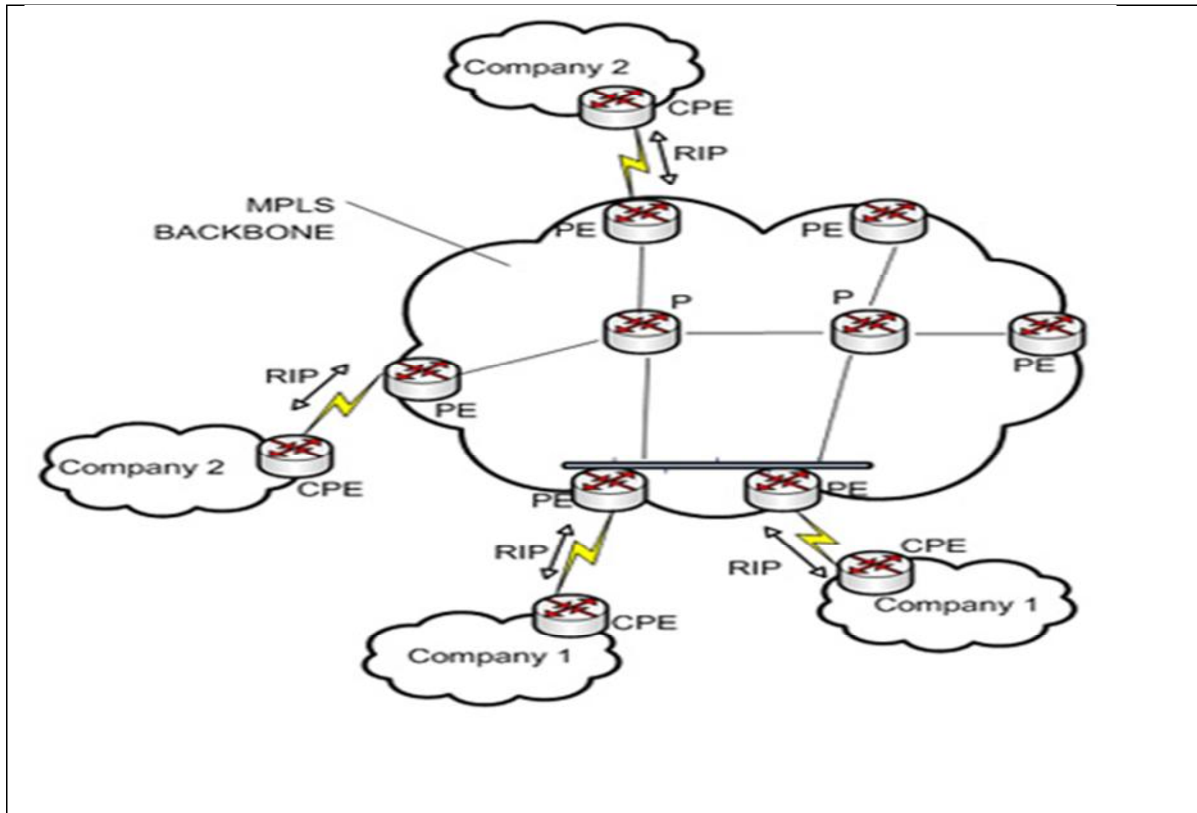



**Figure 1.12 :** récapitulatif VPN/MPLS

## 1.3.6 Comparaison entre MPLS et IPSec.

| | Mpls | Ipsec |
|---|---|---|
| **Qualité de service** | Permet d'attribuer des priorités au trafic par le biais de classes de service | Le transfert se faisant sur l'Internet public, permet seulement un service "best effort" |
| **Coût** | Inférieur à celui des réseaux Frame Relay et Atm mais supérieur à celui des autres Vpn IP. | Faible grâce au transfert via le domaine Internet public |
| **Sécurité** | Comparable à la sécurité offerte par les réseaux Atm et Frame Relay existants. | Sécurité totale grâce à la combinaison de certificats numériques et de Pki pour l'authentification ainsi qu'à une série d'options de cryptage, triple DES et AES notamment |
| **Applications compatibles** | Toutes les applications, y compris les logiciels d'entreprise vitaux exigeant une qualité de service élevée et une faible latence et les applications en temps réel (vidéo et voix sur IP) | Accès à distance et nomade sécurisé. Applications sous IP, notamment courrier électronique et Internet. Inadapté au trafic en temps réel ou à priorité élevée |
| **Etendue** | Dépend du réseau Mpls du fournisseur de services | Très vaste puisque repose sur l'accès à Internet |
| **Evolutivité** | Evolutivité élevée puisque n'exige pas une interconnexion d'égal à égal entre les sites et que les déploiements standard peuvent prendre en charge plusieurs dizaines de milliers de connexions par Vpn | Les déploiements les plus vastes exigent une planification soigneuse pour répondre notamment aux problèmes d'interconnexion site à site et de peering |
| **Frais de gestion du réseau** | Aucun traitement exigé par le routage | Traitements supplémentaires pour le cryptage et le décryptage |
| **Vitesse de déploiement** | Le fournisseur de services doit déployer un routeur Mpls en bordure de réseau pour permettre l&148;accès client | Possibilité d'utiliser l'infrastructure du réseau Ip existant |
| **Prise en charge par le client** | Non requise. Le Mpls est une technologie réseau | Logiciels ou matériels client requis |

**Tableau1.1:** Comparaison entre MPLS et IPSec.

## Conclusion

Cette étude des solutions Vpn, met en évidence une forte concurrence entres les différents protocoles pouvant être utilisés.

Néanmoins, il est possible de distinguer deux rivaux sortant leurs épingles du jeu, à savoir Ipsec et Mpls. Ce dernier est supérieur, mais il assure, en outre, simultanément, la séparation des flux et leur confidentialité. Le développement rapide du marché pourrait bien cependant donner l'avantage au second. En effet, la mise en place de Vpn par Ip entre généralement dans une politique de réduction des coûts liés à l'infrastructure réseau des entreprises. Les Vpn sur Ip permettent en effet de se passer des liaisons louées de type Atm ou Frame Relay. Le coût des Vpn Ip est actuellement assez intéressant pour motiver de nombreuses entreprises à franchir le pas. A performance égales un Vpn Mpls coûte deux fois moins cher qu'une ligne Atm. Mais si les solutions à base de Mpls prennent actuellement le devant face aux technologies Ipsec c'est principalement grâce à l'intégration possible de solution de téléphonie sur Ip. La qualité de service offerte par le Mpls autorise en effet Ce type d'utilisation. Le marché des Vpn profite donc de l'engouement actuel pour ces technologies qui permettent elles aussi de réduire les coûts des infrastructures de communication. Les Vpn sont donc amenés à prendre de plus en plus de place dans les réseaux informatiques.

Chapitre 2 :

---

# Réalisation

---

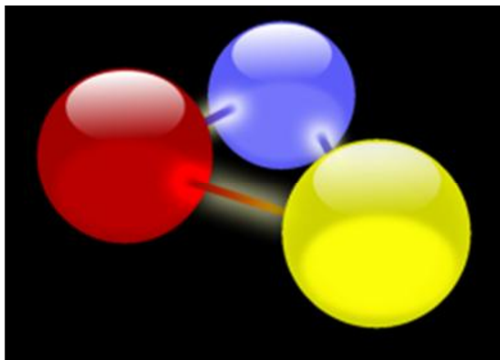
- **Présentation du logiciel GNS3.**
- **Description de la maquette.**
- **Configuration d'un VPN MPLS.**

# Chapitre 2 : Réalisation.

## Introduction.

Nous avons réalisé une maquette simulant la solution MPLS VPN à l'aide de l'émulateur GNS3 de Cisco, une étude a était entamée concernant les différents protocoles de routages et leur configuration sur les routeurs Cisco.

## 2.1 Présentation du logiciel GNS3.



Le logiciel GNS3 est en fait une interface graphique pour l'outil sous-jacent Dynamips qui permet **l'émulation** de machines virtuelles Cisco. Il est nécessaire d'insister sur le terme émulation, dans la mesure où ces machines s'appuient sur les véritables IOS fournis par Cisco et leur confèrent donc l'intégralité des fonctionnalités originales.

Ce logiciel peut donc être opposé à Packet Tracer, qui est un simulateur fourni par Cisco dans le cadre de son programme académique, et qui est donc limité aux seules fonctionnalités implémentées par les développeurs du logiciel.

Les performances des machines ainsi créées ne sont bien entendu pas équivalentes à celles des machines physiques réelles, mais elles restent amplement suffisantes pour mettre en œuvre des configurations relativement basiques et appréhender les concepts de base des équipements Cisco.

A l'heure actuelle, seules certaines plateformes de routeurs sont émulées ainsi que les plateformes PIX et ASA qui sont les Firewalls de la gamme Cisco. De simples commutateurs Ethernet sont émulés, et permettent notamment l'interconnexion du Lab virtuel ainsi crée avec un réseau physique.

Cette solution pourra donc être choisie pour la mise en place de labos virtuels, notamment dans le cadre de la préparation des premières certifications Cisco telles que le CCNA, mais nécessitera une machine avec de bonnes ressources pour émuler plusieurs équipements en simultané.

Pour tout autre renseignement sur le produit ou son téléchargement, vous pouvez vous rendre directement sur la page www.gns3.net . Concernant les IOS, il vous faudra un compte CCO pour télécharger les IOS souhaités depuis le site de Cisco.

## 2.2 Description de la maquette.

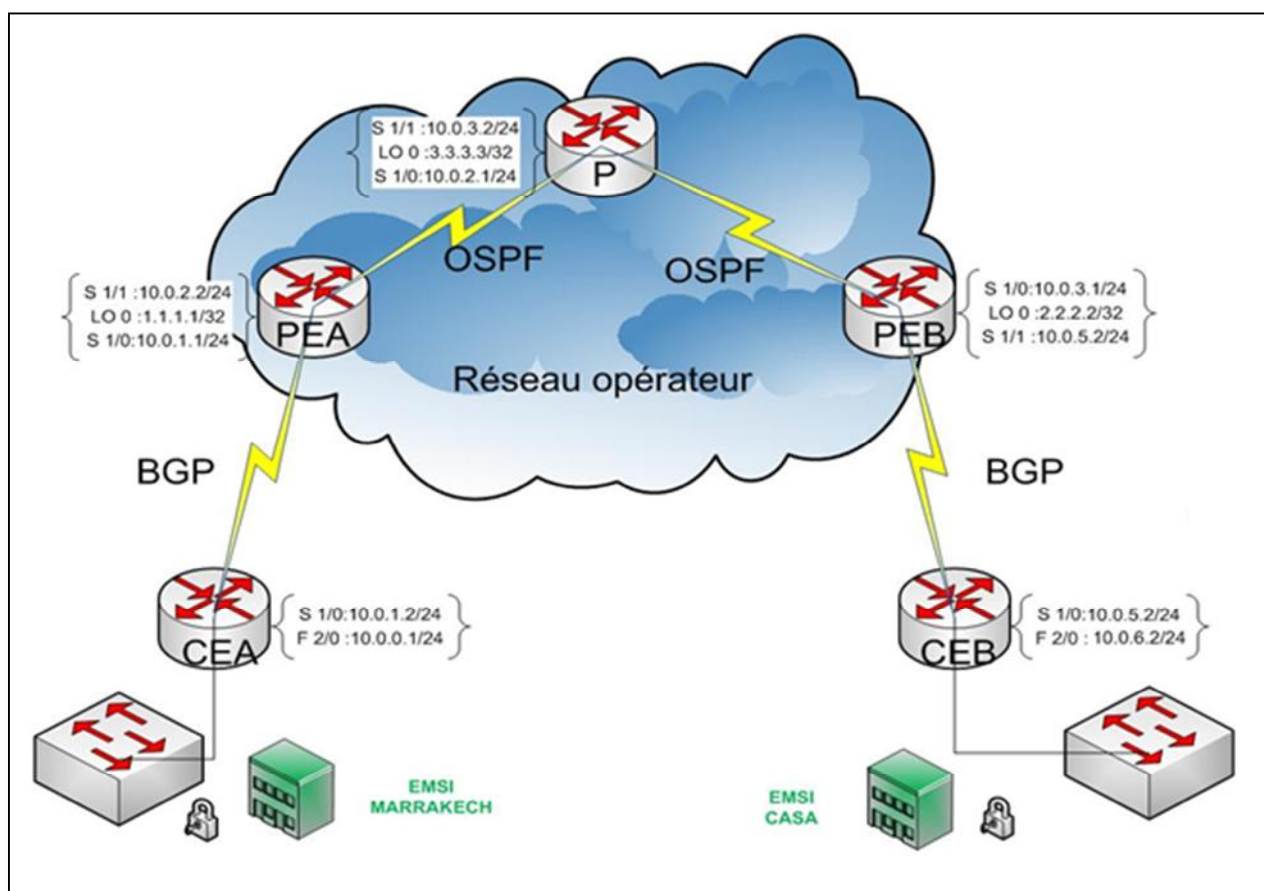



**Figure 2.20:** Maquette réalisée.

Cette topologie met en évidence un VPN d' Intranet simple entre deux sites appartenant au client EMSI : situe A et site B. Le réseau du client comprend les routeurs CEA et CEB.

Nous avons utilisé pour cette tâche 5 routeurs dont :

- ✓ 1 routeur représentant le core MPLS (des routeurs P).
- ✓ 2 routeurs représentant l'edge MPLS (des routeurs PE) et simulant les routeurs de Casa et Marrakech.
- ✓ 2 routeurs désignant des sites de l'EMSI (des routeurs CE).

Tous les routeurs sont de type Cisco, la gamme 7200 utilisant comme image IOS « c7200-jk9o3s-mz.124-19.bin » supportant la technologie MPLS.

## 2.2.1 L'activation du routage

Pour le routage, le protocole OSPF est implémenté dans le backbone, l'exécution du protocole OSPF n'est pas une exigence et n'a aucun effet sur le comportement des routeurs. MPLS VPN offre la possibilité d'utiliser tous types de protocoles de routages pour les sites clients puisque l'échange des routes entre les routeurs PE est réalisé par MP-BGP.

Un autre protocole de routage est activé qui est BGP mais seulement au niveau des routeurs PE pour l'échange des routes MPLS VPN. Les connexions entre les routeurs sont assurées par leurs interfaces séries.

## 2.2.2 L'activation du MPLS

Seulement les routeurs PE et P supportent MPLS donc l'activation est réalisée à ce niveau. Avant de configurer MPLS sur les interfaces des routeurs il est indispensable d'activer le CEF (Cisco Express Forwarding). Le Cisco Express Forwarding (CEF) est une technologie Couche 3 qui fournit une évolutivité de transfert et d'exécution accrus pour gérer plusieurs flux de trafic de courte durée. L'architecture CEF place seulement les préfixes de routage dans ses tables CEF (la seule information qu'elle requiert pour prendre des décisions de transfert Couche 3) se fondant sur les protocoles de routage pour faire le choix de l'itinéraire. En exécutant une consultation de simple table CEF, le routeur transfert les paquets rapidement et indépendamment du nombre de flux transitant.

Nous avons choisit LDP (*Label Distribution Protocol*) pour distribuer les labels MPLS. Comme les interfaces des routeurs dans notre maquette sont de type série.

### 2.2.3 L'activation du MPLS VPN

Nous allons considérer un VPN « emsi ». La première étape est la configuration du MP-BGP sur les routeurs PE (PEA et PEB) pour cela on doit :

- ✓ Activer le protocole BGP sur le routeur avec comme numéro de système autonome 65000.
- ✓ Activer la session BGP VPNv4 entre les deux routeurs PE. Pour pouvoir ajouter un voisin dans la configuration VPNv4, ce voisin doit être préalablement déclaré dans la configuration globale de BGP.

La deuxième étape est la conception (*Design*) VPN caractérisé par le choix des paramètres RD (*Route Distinguisher*) et RT (*Route Target*) qui sont des communautés étendues BGP et définissent l'appartenance aux VPN. La plus simple méthode est d'assigner à chaque VPN le même RD et RT.

## 2.3 Configuration d'un VPN MPLS

Cette partie décrit les configurations génériques exigées sur les routeurs dans le domaine du fournisseur de services, pour mettre en application un VPN basé sur MPLS. Toutes les configurations décrites dans les sections suivantes sont exécutées à partir du réseau montré dans la figure 2.1.

| | |
|---|---|
| **Hostname CEA**<br>**ip cef** | activation du MPLS |
| **interface FastEthernet2/0**<br>**ip address 10.0.0.1 255.255.255.0** | Configuration de l'interface FastEthernet2/0. |
| **interface Serial1/0**<br>**ip address 10.0.1.2 255.255.255.0**<br>**clock rate 2016000** | Configuration de l'interface Serial1/0. |
| **router bgp 65001**<br>**no synchronization**<br>**bgp log-neighbor-changes**<br>**network 10.0.0.0**<br>**redistribute connected**<br>**neighbor 10.0.1.1 remote-as 65000** | Configuration du routage BGP sur le routeur CEA. |

**Tableau 2.2:** Configuration du routeur CEA





| | |
|---|---|
| **hostname PEA**<br>**ip cef** | Attribution du nom au routeur.<br>Activation du MPLS. |
| **ip vrf emsi**<br>**rd 100:100**<br>**route-target both 100:100** | **Configurer VRF sur le routeur PE :**<br>le VRF emsi sur le routeur PEA et PEB. Ceci a comme conséquence la création d'une table de routage VRF et d'une table emsi Express Forwarding (CEF) pour emsi. Cet exemple montre emsi VRF étant configuré sur le routeur PEA. Notez que le nom de VRF est sensible à la casse.<br>**Configurer le RD:**<br>Le RD crée des tables de routage et de transmission. Le RD est ajouté au début des en-têtes IPv4 du client pour les convertir en préfixes globalement uniques VPNv4.<br>**Configuration des paramètres VRF: RT**<br>Configurer l'importation et l'exportation des stratégies: Configurent l'importation et l'exportation de stratégies pour les communautés MP-BGP. La stratégie est employée pour filtrer des itinéraires pour ce "target-route" particulière.<br>PEA(config-vrf)#route-target both 100:100 |
| **interface Loopback0**<br>**ip address 1.1.1.1 255.255.255.255** | Définition de l'adresse pour l'interface Loopback. |
| **interface Serial1/1**<br>**ip address 10.0.2.2 255.255.255.0**<br>**mpls label protocol ldp**<br>**mpls ip**<br>**clock rate 2016000** | mpls ip (sur les interfaces internes des routeurs opérateurs). |
| **interface Serial1/0**<br>**ip vrf forwarding emsi**<br>**ip address 10.0.1.1 255.255.255.0**<br>**clock rate 2016000** | Associer VRF avec une interface<br>Association de VRF à l'adresse IP de l'interface.<br>ip address affecter l'adresse APRES la VRF. |
| **router ospf 1**<br>**network 1.1.1.1 0.0.0.0 area 0**<br>**network 10.0.4.2 0.0.0.0 area 0** | Configuration de ospf entre les PE. |
| **router bgp 65000**<br>**no synchronization**<br>**bgp log-neighbor-changes**<br>**neighbor 2.2.2.2 remote-as 65000**<br>**neighbor 2.2.2.2 update-source Loopback0**<br>**no auto-summary** | Configuration des voisins MP-iBGP.<br><br><br><br>utiliser loopback comme adresse source |
| **address-family vpnv4**<br>**neighbor 2.2.2.2 activate**<br>**neighbor 2.2.2.2 send-community both**<br>**neighbor 2.2.2.2 next-hop-self**<br>**exit-address-family** | Configuration de l' "address-familiy" BGP VPNv4<br>activer les familles d'adresses IPv4 et vpnv4 |
| **address-family ipv4 vrf emsi**<br>**neighbor 10.0.1.2 remote-as 65001**<br>**neighbor 10.0.1.2 activate**<br>**neighbor 10.0.1.2 as-override** | Configuration de BGP par VRF IPv4 (Contexte de routage) |

**Tableau 2.3:** Configuration du routeur PEA





| | |
|---|---|
| **hostname PEB**<br>**ip cef** | activation du MPLS |
| **ip vrf emsi**<br>**rd 100:100**<br>**route-target both 100:100** | . |
| **interface Loopback0**<br>**ip address 2.2.2.2 255.255.255.255** | |
| **interface Serial1/0**<br>**ip address 10.0.3.1 255.255.255.0**<br>**mpls label protocol ldp**<br>**mpls ip**<br>**clock rate 2016000** | |
| **interface Serial1/1**<br>**ip vrf forwarding emsi**<br>**ip address 10.0.5.2 255.255.255.0**<br>**clock rate 2016000** | |
| **router ospf 1**<br>**network 2.2.2.2 0.0.0.0 area 0**<br>**network 10.0.4.1 0.0.0.0 area 0** | |
| **router bgp 65000**<br>**no synchronization**<br>**bgp log-neighbor-changes**<br>**redistribute connected**<br>**neighbor 1.1.1.1 remote-as 65000**<br>**neighbor 1.1.1.1 update-source Loopback0**<br>**no auto-summary** | |
| **address-family vpnv4**<br>**neighbor 1.1.1.1 activate**<br>**neighbor 1.1.1.1 send-community both**<br>**neighbor 1.1.1.1 next-hop-self**<br>**exit-address-family** | |
| **address-family ipv4 vrf emsi**<br>**neighbor 10.0.5.1 remote-as 65001**<br>**neighbor 10.0.5.1 activate**<br>**neighbor 10.0.5.1 as-override**<br>**no synchronization**<br>**exit-address-family** | |

**Tableau 2.4:** Configuration du routeur PEB

| | |
|---|---|
| **hostname CEB**<br>**ip cef** | activation du MPLS. |
| **interface FastEthernet2/0**<br>**ip address 10.0.6.2 255.255.255.0** | Configuration de l'interface FastEthernet2/0. |
| **interface Serial1/0**<br>**ip address 10.0.5.1 255.255.255.0**<br>**clock rate 2016000** | Configuration de l'interface Serial1/0. |
| **router bgp 65001**<br>**no synchronization**<br>**bgp log-neighbor-changes**<br>**network 10.0.0.0**<br>**redistribute connected**<br>**neighbor 10.0.5.2 remote-as 65000**<br>**no auto-summary** | **Configuration du routage BGP sur le routeur CEB.** |

**Tableau 2.5 :** Configuration du routeur **C**EB

| | |
|---|---|
| **hostname P**<br>**ip cef** | Activation du MPLS |
| **interface Loopback0**<br>**ip address 3.3.3.3 255.255.255.255** | . |
| **interface Serial1/0**<br>**ip address 10.0.2.1 255.255.255.0**<br>**mpls label protocol ldp**<br>**mpls ip**<br>**clock rate 2016000** | |
| **interface Serial1/1**<br>**ip address 10.0.3.2 255.255.255.0**<br>**mpls label protocol ldp**<br>**mpls ip**<br>**clock rate 2016000** | |
| **router ospf 1**<br>**network 3.3.3.3 0.0.0.0 area 0**<br>**network 10.0.2.1 0.0.0.0 area 0**<br>**network 10.0.3.2 0.0.0.0 area 0** | |

**Tableau 2.6:** Configuration du routeur P.

## Verification:

- **show ip vrf** vérifies l´existence de la table VFR.
- **show ip vrf interfaces** Vérifies les interfaces actives.
- **show ip route vrf emsi** Vérifies les informations de routage au niveau du routeur PE.
- **traceroute vrf emsi 10.0.0.1** Vérifies les informations de routage au niveau du routeur PE.
- **show ip bgp vpnv4 tag** : Vérifie le protocole de routage BGP.
- **show ip cef vrf emsi 10.0.0.1 detail** : Vérifie les informations de routage au niveau du routeur PE.
- **sh mpls forwarding-table**
- **sh tag-switching tdp bindings**
- **sh ip ospf database**
- **sh ip route**

```
CEB#traceroute 10.0.0.1

Type escape sequence to abort.
Tracing the route to 10.0.0.1

  1 10.0.5.2 140 msec 148 msec 192 msec
  2 10.0.3.2 [MPLS: Labels 16/19 Exp 0] 984 msec 920 msec 864 msec
  3 10.0.1.1 [AS 65000] [MPLS: Label 19 Exp 0] 764 msec 692 msec 516 msec
  4 10.0.1.2 [AS 65000] 912 msec 972 msec 1096 msec
CEB#
```

**Figure 2.21:** Commande « traceroute » exécutée au niveau du routeur CEB avec l'adresse 10.0.0.1

Le label MPLS affiché pour chaque hop correspond au label en entrée du routeur. Le champ « Exp » (codé sur 3 bits) est similaire au champ TOS de l'entête IP, mais n'est pas employé ici.

Le routeur PEB a inséré 2 Labels dans le paquet, le premier label (19) pour le VPN « emsi », le deuxième (16) pour la commutation LSP au sein du nuage MPLS.

Le routeur P a supprimé le Label (16) du paquet avant de le réexpédier au routeur PEA.





```
CEA#traceroute 10.0.6.2

Type escape sequence to abort.
Tracing the route to 10.0.6.2

  1 10.0.1.1 296 msec 136 msec 324 msec
  2 10.0.2.1 [MPLS: Labels 17/19 Exp 0] 1420 msec 984 msec 992 msec
  3 10.0.5.2 [AS 65000] [MPLS: Label 19 Exp 0] 704 msec 472 msec 512 msec
  4 10.0.5.1 [AS 65000] 744 msec 1020 msec 772 msec
CEA#
```

**Figure 2.22:** Commande « traceroute » exécutée au niveau du routeur CEA avec l'adresse 10.0.6.2

Le label MPLS affiché pour chaque hop correspond au label en entrée du routeur. Le champ « Exp » (codé sur 3 bits) est similaire au champ TOS de l'entête IP, mais n'est pas employé ici.

Le routeur PEA a inséré 2 Labels dans le paquet, le premier label (19) pour le VPN « emsi », le deuxième (17) pour le routeur lui-même.

Le routeur P a supprimé le Label (17) du paquet avant de le réexpédier au routeur PEB.

```
PEB#show ip vrf
  Name                                  Default RD
        Interfaces
  emsi                                  100:100
        Se1/1
```

**Figure 2.23:** Commande « Show ip vrf » exécutée au niveau du routeur PEB.

La commande ' Show ip vrf ' permet de tester l'existence des VRFs sur l'ensemble des interfaces d'un routeur, et les affichées.

Dans notre exemple, le nom du vrf est ' emsi ' sur l'interface série 1/1.

```
PEA#show ip vrf interfaces
Interface          IP-Address      VRF                    Protocol
Se1/0              10.0.1.1        emsi                   up
PEA#
```

**Figure 2.24**: Commande « Show ip vrf interfaces » exécutée au niveau du routeur PEA.

Cette commande permet d'afficher l'interface sur laquelle le VRF est activé, ici c'est l'interface Série 1/0 avec comme adresse IP : 10.0.1.1





```
PEB#sh mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     16          1.1.1.1/32        0          Se1/0      point2point
17     Pop tag     3.3.3.3/32        0          Se1/0      point2point
18     Pop tag     10.0.2.0/24       0          Se1/0      point2point
19     Untagged    10.0.6.0/24[V]    0          Se1/1      point2point
20     Aggregate   10.0.5.0/24[V]    1224
PEB#
```

**Figure 2.25:** Commande « Show mpls forwarding-table » exécutée au niveau du routeur PEB.

Cette commande permet de voir le LFIB de PEB constitué dynamiquement grâce au protocole LDP.

```
PEA#show ip cef vrf emsi 10.0.6.2 detail
10.0.6.0/24, version 18, epoch 0, cached adjacency to Serial1/1
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Se1/1, point2point, tags imposed: {17 19}
  via 2.2.2.2, 0 dependencies, recursive
    next hop 10.0.2.1, Serial1/1 via 2.2.2.2/32
    valid cached adjacency
    tag rewrite with Se1/1, point2point, tags imposed: {17 19}
PEA#
```

**Figure 2.26:** Commande « Show ip cef vrf emsi 10.0.6.2 detail » exécutée au niveau du routeur PEA.

La table CEF d'une VRF peut également être examinée, au moyen de la commande « *show ip cef vrf emsi* »

## Conclusion :

Dans ce chapitre, nous avons, tous d'abord, présenté l'émulateur GNS3 de CISCO. Il est à signaler que nous avons pu parvenir à utiliser un IOS (Image Shell des routeurs CISCO) récent après des multiples difficultés que nous avons pu surmonter en s'appuyant sur plusieurs profondes recherches ainsi qu´une documentation très difficile à trouver.

En dernier, nous avons choisi une topologie réseau permettant de mettre en œuvre les principales fonctionnalités VPN MPLS. Une topologie qui consiste à interconnecter les deux sites EMSI via un réseau opérateur utilisant comme technologie de transport MPLS.

Les résultats escomptés sont commentés et montrent bien le fonctionnement de notre réseau.

# Conclusion Générale

L'évolution dans le domaine des télécommunications ne cesse de donner une grande souplesse pour trouver des solutions efficaces pour certains dangers et pour fournir une sécurité des biens et des personnes. En effet, la combinaison entre les technologies VPN et MPLS a permis de fournir une solution sécuritaire. Cette solution assure, d'une manière efficace, la protection des biens et des personnes n'importe où dans le monde.

Ce rapport s'articule sur deux chapitres : dans le premier, nous avons exposé les fondements des VPNs, Dans le deuxième, nous avons présenté une solution VPN d'Intranet simple entre deux sites appartenant au client EMSI.

Comme perspective de ce travail, nous proposons une solution mixte VPN MPLS/IPSec. La nouvelle solution, intégrant une partie des solutions réseaux existantes, est composée d'un réseau VPN/MPLS reliant les « PE, P » associés à des accès IPSec pour les sites qui s'y rattachent, afin de rendre le réseau plus sécurisé.

# Bibliographie


(1) **GUY PUJOLLE,** « Les Réseaux », 6éme édition, EYROLLES, 2008, numéros des pages consultées [853-866].

(2) **R. et E. Corvalan et Y,** « Les VPN», DUNOD.

(3) **Bibliographie WEB :**

- http://www.securiteinfo.com/
- http://www.hsc.fr/
- http://www.routage.org/
- www.cisco.com
- www.ietf.org
- WWW.GNS3.com






# Annexes

Table de routage:

```
CEB#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile,
 B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA -
OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
       E1 - OSPF external type 1, E2 - OSPF external t
ype 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level
-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U
 - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 4 subnets
B       10.0.0.0 [20/0] via 10.0.5.2, 00:12:42
B       10.0.1.0 [20/0] via 10.0.5.2, 00:12:42
C       10.0.6.0 is directly connected, FastEthernet2/
0
C       10.0.5.0 is directly connected, Serial1/0
CEB#
```

Verifier le BGP:

```
PEB#show ip bgp vpnv4 all
BGP table version is 8, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:100 (default for vrf emsi)
*>i10.0.0.0/24      1.1.1.1                  0    100      0 65001 ?
*>i10.0.1.0/24      1.1.1.1                  0    100      0 65001 ?
r> 10.0.5.0/24      10.0.5.1                 0             0 65001 ?
*> 10.0.6.0/24      10.0.5.1                 0             0 65001 ?
PEB#
```

Verifier l'OSPF:

```
PEA#sh ip ospf database

            OSPF Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         1102        0x80000004 0x002836 3
2.2.2.2         2.2.2.2         1103        0x80000004 0x0072DE 3
3.3.3.3         3.3.3.3         1098        0x80000002 0x008B03 5
PEA#
```





| *Commande Cisco* | *Description* |
|---|---|
| **router (config) # router OSPF *process-id*** | activer le protocole OSPF sur le routeur avec le choix d'un numéro de processus. |
| **router (config) # router OSPF *process-id* vrf** *vrf-name* | Activer le protocole OSPF avec une vrf particulière |
| **router (config-router) # network *address wildcard-mask* area *area-id*** | ajouter un réseau pour le routage OSPF.<br>*Address :* Peut être une adresse réseau, sous réseau ou une adresse d'interface<br>*wildcard-mask :* C'est le masque générique<br>*Area-id :* Spécifier l'area associé à l'adresse |
| **router (config) # router BGP *as-number*** | activer le protocole de routage en spécifiant le nombre du système autonome. |
| **router (config-router) # Address-family ipv4 vrf** *vrf-name* | sélectionner du protocole de routage une instance de VRF. |
| **router (config-router) # Address-family vpnv4** | sélection de la configuration d'une VRF pour le protocole de routage BGP |
| **router (config-if) # Ip vrf forwarding *vrf-name*** | Assigner une l'interface à une VRF |
| **router (config) # Ip vrf *vrf-name*** | Créer une VRF |
| **router (config-router-af) # Neighbour *ip-address* activate** | Activer l'échange des routes vpnv4 avec le voisin spécifié |
| **router (config-router-af) # Neighbour *ip-address* next-hop-self** | Configurer le routeur comme le saut suivant pour le protocole BGP |
| **router (config-router) # Neighbour *ip-address* remote-as** | Ajouter une entrée dans la liste des voisins pour MP - BGP |
| **router (config-router-af) # Neighbour *ip-address* send-community both** | Spécifier la nature de la communité qui doit être envoyée au voisin BGP |
| **router (config-router) # Neighbour *ip-address* update-source** | Permettre la session IBGP d'utiliser n'importe quelle interface opérationnelle pour les connexions TCP |
| **router (config-vrf) # Rd *value*** | Assigner un RD à une VRF |
| **router(config-vrf) # Route-target import \| export *value*** | Assigner un RT à une VRF |
| **router (config) # ip cef** | permettre l'utilisation de la technique de commutation Cisco Express Forwading (CEF). |
| **router (config-subif) # mpls ip** | activer la commutation MPLS |
| **router (config-subif) # mpls label protocol {ldp \| tdp \| both}** | spécifier le protocole de distribution de label sur l'interface approprié. |
| **router (config) # redistribute bgp** *as-number* **subnets** | Redistribuer les routes BGP (incluant celles des sous réseaux) en OSPF |